INFORMATION HIDING METHOD WITH REDUCED FUZZINESS

BACKGROUND OF THE INVENTION

Field of Invention

The present invention relates to an information hiding method and, in particular, to an information hiding method with reduced fuzziness.

Related Art

Owing to the rapid development in computer network technology, the whole world has entered the digital era. This has made information communications and knowledge sharing much easier. However, the issue of security over the network gradually threatens the efforts in protecting network intellectual properties. The applications of computer networks in national defense, such as the information systems in command, management, communications and intelligence or modern weapon equipment, are more and more popular. Therefore, how classified information can acquire safety authenticates on the network has become an urgent problem to be solved. Practically speaking, the so-called electronic signature technology refers to the techniques that prevent unintended users from eavesdropping, copying and modifying others' information so that the legal user can extract authenticated information from a meaningful image. This is the so-called steganography.

By steganography refers to embedding a portion of meaningful texts, image or video signal irrelevant to the image being transmitted during the image transmission. It is made to be hard for an unauthorized third party to see whether there is hidden information or not in the transmission process. This can prevent hackers from damaging the transmitted information. A common method seen in the steganography is to select a host image, to hide therein some information and thus to generate another watermarked image. This image looks just like the host image by naked eyes, and it is hard to find out directly that other information is contained therein. Other users on the network cannot determine whether this signed image contains other information or not. Thus, from all the information on the network unauthorized users are unable to distinguish electronically signed images from unsigned ones. However, a legal user can readily extract the hidden electronic signature from the transmitted information.

Normally, the steganography must have the following features:

1. Undetectable: The electronic signature is hidden behind the image information so that it would not be found using usual image processing methods;
2. Invisible: An image attached with the electronic signature looks the same as the host image by naked eyes;
3. Undeletable: The electrical signature added to the image cannot be easily deleted using simple image processing methods;
4. Resistant to image manipulation: The electrical signature is not susceptible to damages caused by normal image processing or on purpose.

The steganography has the space and frequency domains. In the research field of the frequency domain, using frequency expansions on the electronic signature is fine but has the following three disadvantages:

1. The computation is too tedious. Conversion to the frequency domain requires complicated calculation. The receiver end also needs the corresponding converter. This is inconvenient to applications that demand real time processing.
2. It is vulnerable to attacks. Most hiding methods in the frequency domain hide the information in peripheral sections to avoid damages caused by fuzziness compression. Therefore, it is easy for invaders to attack the hidden information.
3. It can hide relatively little information. The information can only be hidden within a specific frequency band in the frequency domain, so it can hide relatively little information.

In the space domain, a commonly employed information hiding method is the vector quantization. It uses a code book commonly owned by both the sender and the receiver to encode the electronic signature. Over the sender end, the sender cuts the electronic signature to be hidden into the same size as the blocks in the code book, finds a similar block from the code book and hides in the image its index in place of the information in this block, and finally sends it to the network. Over the receiver end, when the receiver receives the image with hidden information he decodes the index, looks it up in the code book and restores the information. The defect of this method is that there is larger information fuzziness and that the image with hidden information cannot withstand the

damages caused by fuzziness.

Another steganography uses fixed areas in image pixels to hide information, *e.g.*, the fixed range equalization method. The gray scale of the image to hide information in this method is divided into 16 sections. The hidden information, in unit of bytes, replaces the original value at a point depending upon the space the input value belongs to. For example, if the information has a value of 17, then one point within the range from 16~31 is thus replaced by 17. There is yet another method called LSB, which is also often used for hiding information. LSB places the electronic signature in the lower (less important) bytes because the change in lower bytes has less impact on the whole pixel values and thus has less obvious damages to the image. Nevertheless, the above two methods cannot withstand the fuzziness damages after the image is hidden with information. Other references provide some ingenious methods for hiding information, but none of them can provide an effect solution to human damages.

SUMMARY OF THE INVENTION

The present invention provides a method for hiding information using several communications and image processing techniques. First, the B channel in the RGB color image is selected to hide information because human eyes are not sensitive to the B channel. The information is then embedded therein using ~~cross~~interleaving encoding, channel encoding and pixel location correlation. With the encoding/decoding techniques and the comparison among neighboring pixels, the hidden information can be effectively protected from illegal modification. Also, because of the restoration ability of the channel encoding and the comparison among neighboring pixels, the present invention can correctly restore the information even after JPEG fuzziness compression.

The disclosed method can protect the information and withstand fuzziness damages. Using the channel encoding technique and the image correlations, a method of producing an electronic signature is provided by further combining with some basic image hiding techniques. This invention has practical values in determining the belonging of copyrights and information camouflage.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will become more fully understood from the detailed description given hereinbelow illustration only, and thus are not limitative of the present invention, and

wherein:

FIG. **1** is a flow chart of the method for hiding information according to the present invention;

FIG. **2** is a functional diagram of input and output using ~~spin~~convolutional codes according to the present invention;

FIG. **3** is a schematic view of the hardware circuit in the ~~cross~~interleaving code generator according to the present invention;

FIG. **4** shows a state of a random number sequence in the buffer of the present invention;

FIG. **5** is a diagram showing the locations of information embedding point and its peripheral relevant pixels during information embedding according to the present invention;

FIG. **6** is a flow chart of the method for extracting the hidden information according to the present invention;

FIG.~~Attachment~~ 7-**1** is a host image;

FIG. 7-~~Attachment~~-**2** is the information to be hidden;

FIG. 7-~~Attachment~~-**3** is the image after embedding information; and

FIG. 7-~~Attachment~~-**4** is the image after human damages.

DETAILED DESCRIPTION OF THE INVENTION

The host image, H, for hiding information in the present invention is an image composed of three m×n pixels of R, G, B colors, respectively, the value of each pixel ranging from 0 to 255. The information to be hidden in the host image is a bit series with L bits. So the host image H and the embedded image W are:

$$H=\{h_{ij} \mid 0 \leqq i < m, 0 \leqq j < n, h_{ij} \in [0,255]\},$$

$$W=\{w_i \mid 0 \leqq i < l, w_i \in [0,1]\}.$$

A set $ASET_{ij}=\{h_{i+1,j}, h_{i-1,j+1}, h_{i,j+1}, h_{i+1,j+1}\}$ is defined for the four pixels that surround any pixel h_{ij} in the host image on the right hand side.

The flow chart of the method for hiding information disclosed herein is shown in FIG. 1. It consists of three steps: ~~spin~~convolutional encoding (step **10**), ~~cross~~ interleaving encoding (step **20**) and embedding information into the image (step **30**). The process is

done to the B channel. After the three steps are completed, the image embedded with the information is transmitted (step **40**).

In the first step of ~~spin~~convolutional encoding, the ~~spin~~convolutional encoding is a type of channel encoding. The purpose of the channel encoding is to make the encoded information free from noises during transmission. Using the feature of embedding information in the host image, the size of the image would not be increased after channel encoding and it can be restored even after image compression or human damages. In practice, the (2,1,7) ~~spin~~convolutional codes are employed to generate information that is twice that of the embedded information using a ~~spin~~convolutional encoder. The extra encoding information is used to correct the transmission errors or human damages. By (2,1,7), the first component 2 means that the encoded output is in 2 bits, the second component 1 means that the input information is in 1 bit, and the third component 7 means that there are 6 (=7-1) buffers. ~~Spin~~Convolutional codes of different complexities can be used on different hardware. If the hardware can provide greater computation power, a more complicated ~~spin~~convolutional encoder can be used to obtain a better anti-interference effect. FIG. **2** is a functional diagram of input and output using ~~spin~~convolutional code according to the present invention, wherein the hardware structure has two buffers **50,52** for the ~~spin~~convolutional code (2,1,3).

In the second step of performing ~~cross~~interleaving encoding, the random number generator of a linear feedback shift register generates a set of so-called m-sequence random numbers. The seed used is taken as a private key, the first key to information restoration. The receiver has to have this key to extract the information. If the information is in 8 bits, the key can be ~~cross~~interleaving generated using the hardware shown in FIG. **3**, which is a schematic view of the hardware circuit in the ~~cross~~interleaving code generator according to the present invention. The feedback function is f(x1,x2,x3)=x1+x3, which can generate a random number sequence with a cycle of 7. The state of the random number sequence is shown in FIG. **4**. The digital information such as (010) in FIG. **4** represents the contents of buffers **54,56,58** in FIG. **3**. Different initial values can be different seeds for generating random numbers of different orders. These different orders are used to permute the 8 bits of information for ~~cross~~interleaving effects. Since the present method has a greater

randomness than the conventional ~~cross~~interleaving methods (matrix), does not need to store the whole table, and needs only one initial value, large memory space can be saved.

The third step of information embedding comprises location selection and information embedding. A proper location is selected from the host image and then the information is hidden therein. When each bit of the information is added into the host image, the pixels around the host image are processed first. The present invention uses a random number generator to "play dice" for the host image from left to right and from top to bottom. If the dice playing wins, that pixel of the host image is selected as one information embedding point. If the pixel h_{ij} is an information embedding point, the positions of the surrounding pixels are as shown in FIG. 5.

The percentage of the random number generator determines L positions (or its multiples, depending upon the character of the ~~spin~~convolutional code) as the information embedding points. For example, if the random number generator generates numbers between 1 through 10 and the number of bits of the information to be embedded is 30% of the total number of pixels in the B channel of the host image, then whenever 1, 2 or 3 is obtained in the dice-playing, this pixel is considered as an information embedding point; otherwise, the system processes the next pixel. The seed of the random numbers is taken as a second key to extract the information (the hidden electronic signature).

After ~~spin~~convolutionalning encoding, the embedded information is multiplied by L. For example, the (2,1,7) encoding would make L-bit information into 2L-bit information. If the current bit to be inserted is w and the information embedding point in the host image is h_{ij}, then a temporary variable h' is calculated as follows:

$$h'=(h_{i-1,j-1}+h_{i,j-1}+h_{i-1,j+1}+h_{i-1,j}+h_{i+1,j}+h_{i-,j+1}+h_{i,j+1}+h_{i+1,j+1})/8,$$

The values of $h_{i,j}$ and $ASET_{i,j}$ are adjusted according to the following algorithm:

```
while(((h'-hij≦t) and (w=0)) or ((hij-h'≦t) and (w=1))) do
begin
for each hi'j' ∈ ASETi,j do
hi'j'=hi'j'-2w+1;
hi,j= hi,j+2w-1;
h'=(hi-1,j-1+hi,j-1+hi-1,j+1+hi-1,j+hi+1,j+hi-,j+1+hi,j+1+hi+1,j+1)/8;
```

end;

Through all the above pixel calculation, the information can be successfully embedded into the image.

FIG. 6 is a flow chart of the method for extracting the information according to the present invention. When the image is transmitted to and received by the receiver(step 60), the information can be extracted by reversing the steps in the above-mentioned method of embedding information(step 70). In the step of extracting information, the positions of hiding the information are calculated using the second key. For each information embedding point $h_{i,j}$, h' is obtained as when embedding the information:

$$h'=(h_{i-1,j-1}+h_{i,j-1}+h_{i-1,j+1}+h_{i-1,j}+h_{i+1,j}+h_{i-,j+1}+h_{i,j+1}+h_{i+1,j+1})/8;$$

and the corresponding information at this position is extracted using

$w=1$ if $h' \leqq h_{i,j}$,

$w=0$ otherwise.

When each bit of information is restored in order, the whole information is sent for ~~cross~~ interleaving decoding(step 80).

In the ~~spin~~convolutional decoding process, the Viterbi algorithm is employed to correct the information with errors. The trellis diagram used for ~~spin~~convolutional decoding can be built up in advance to save the time in information restoration.

The last step in information extraction uses the first key in the information embedding to rebuild the shuffled information. This key is the seed used by the random number generator of the linear feedback shift register in ~~cross~~ convolutional encoding. This seed is used again to run the random number generator in order to reconstruct the information before convolutional~~cross~~ encoding(step 90).

Through the verification by Figs.~~Attachments~~ 7-1~~1~~ through 7-4~~4~~, the human damaged or JPEG compressed host image that has been embedded with hidden information o can still be restored. In addition to successfully restoring information, the original image and the information-embedded image (fake image) have to be indistinguishable by naked eyes. A commonly used peak signal to noise ratio (PSNR) in the image compression technology is a good means to measure visual errors:

$$PSNR = 10\log_{10}\frac{255^2}{MSE}dB,$$

where MSE is the mean square error between the two images in comparison. It is the sum of the squares of the differences between all pairs of two corresponding pixels in the two images divided by the number of total pixels. In general, it is hard for human eyes to distinguish two images when PSNR is over 30dB. The PSNR values for the images in the Attachments are over 35dB, so they are indistinguishable by eyes.

Effect of the Invention

The information hiding method with reduced fuzziness disclosed herein can achieve the following effects:

1. By distributing hidden information, the embedded image is hard to be detected.
2. The B channel is used to store information, so naked eyes cannot recognize.
3. The information cannot be easily removed under the protection of random codes.
4. The ~~spin~~convolutional encoding can correct possible errors during transmission.
5. The ~~cross~~interleaving encoding can fully randomize the information and avoid the occurrence of burst errors.
6. By information embedding, neighboring points share part of the information hidden in a single pixel. Therefore, the method can fight against single point damages and it is not easy for the host image to be ruined due to information distribution.

Two keys are employed to prevent unauthorized persons from eavesdropping and cracking. The method of the present invention provides a secure transmission for the network.

The invention being thus described, it will be obvious that the same may be varied in many ways. Such variations are not to be regarded as a departure from the spirit and scope of the invention, and all such modifications as would be obvious to one skilled in the art are intended to be included within the scope of the following claims.

CLAIMS

What is claimed is:

1. An information hiding method with reduced fuzziness, which comprises the steps of:

   inputting the information to be embedded into a ~~spin~~convolutional encoder and generating encoded information whose length is a multiple of the original information;

   generating a random number sequence using ~~cross~~interleaving encoding for permuting the encoded information, the seed of the random numbers being a first key;

   selecting a pixel of a host image using a random number generator as an information embedding point of the encoded information, the seed of the random number generator being a second key, and

   embedding the encoded information into ~~the~~ a B channel of the pixel of the host image.

2. The method according to claim 1, wherein the ~~spin~~convolutional encoding corrects transmission errors or human damages on the encoded information.
3. The method according to claim 1, wherein the random number sequence is generated by a linear feedback shift register.
4. The method according to claim 3, wherein the linear feedback shift register comprises a plurality of buffers.
5. The method according to claim 1 further comprising the following steps for extracting the embedded information:

   using the second key to compute the embedding positions of the encoded information;

   using the first key to reconstruct the encoded information and to restore the order before ~~cross~~interleaving encoding; and

   decoding the encoded information using ~~spin~~convolutional decoding.

6. The method according to claim 1, wherein the host image H is an image of m×n pixels and the electronic signature to be embedded is information W with a size L,

both the host image H and the embedded information W being expressed as:

$H=\{h_{ij} \mid 0 \leqq i < m, 0 \leqq j < n, h_{ij} \in [0,255]\}$, and

$W=\{w_i \mid 0 \leqq i < L, w_i \in [0,1]\}$; and

a set $ASET_{ij}=\{h_{i+1,j}, h_{i-1,j+1}, h_{i,j+1}, h_{i+1,j+1}\}$ being defined for four pixels surrounding and to the right of any pixel h_{ij} in the host image.

7. The method according to claim 6, wherein a temporary variable is defined to be $h'=(h_{i-1,j-1}+h_{i,j-1}+h_{i-1,j+1}+h_{i-1,j}+h_{i+1,j}+h_{i-,j+1}+h_{i,j+1}+h_{i+1,j+1})/8$.

8. ~~The method according to claim 6 further comprising the step of adjusting the values of $h_{i,j}$ and $ASET_{i,j}$ according to:~~

~~while((($h'-h_{ij} \leqq t$) and ($w=0$)) or (($h_{ij}-h' \leqq t$) and ($w=1$))) do~~

~~begin~~

~~for each $h_{i,j} \in ASET_{i,j}$ do~~

~~$h_{i,j}=h_{i,j}-2w+1$;~~

~~$h_{i,j}= h_{i,j}+2w-1$;~~

~~$h'=(h_{i-1,j-1}+h_{i,j-1}+h_{i-1,j+1}+h_{i-1,j}+h_{i+1,j}+h_{i-,j+1}+h_{i,j+1}+h_{i+1,j+1})/8$;~~

~~end.~~

9. The method according to claim 5, wherein the hidden information is true if $h' \leqq h_{i,j}$ in the step of using the second key to compute the embedding positions of the encoded information.

10. The method according to claim 5, wherein the ~~spin~~convolutional decoding adopts the Viterbi algorithm.

ABSTRACT OF THE DISCLOSURE

An information hiding method with reduced fuzziness, which employs ~~cross~~interleaving encoding, ~~spin~~convolutional encoding and contrasts among neighboring pixels. Once the information is hidden, it can still be extracted without the original image from the generated image after a certain extent of fuzziness damage.

步驟 10 ~~SPIN~~CONVOLUTIONAL ENCODE

步驟 20 ~~CROSS~~INTERLEAVING ENCODE

步驟 30 EMBED INFORMATION INTO IMAGE

步驟 40TRANSMIT

50,52,54,56,58 BUFFER

步驟 60 RECEIVE

步驟 70 IMAGE WITH HIDDEN INFORMATION

步驟 80 ~~CROSS~~INTERLEAVING DECODE

步驟 90 ~~SPIN~~CONVOLUTIONAL DECODE TO OBTAIN INFORMATION